РЕАЛИЗАЦИЯ КОРПОРАТИВНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ВУЗА НА БАЗЕ ТЕХНОЛОГИИ ACTIVE DIRECTORY

В.В. Крюков, В.С. Майоров, К.И. Шахгельдян
Владивостокский государственный университет экономики и сервиса, г.Владивосток

Анализ требований к типовой сетевой инфраструктуре вуза показывает, что без изменения методологии построения сети трудно обеспечить необходимое качество сетевых и телематических сервисов. Сетевая инфраструктура организации является ключевой компонентой, требования к которой изменяются по мере изменения масштаба сети, расширения диапазона информационных сервисов и их качества. Кроме того, сегодня стоит задача перехода от некоторого слабосвязанного набора корпоративных сетей к частной региональной сети с единой политикой управления для покрытия информационными сервисами сложной организационной структуры современного вуза с территориально распределенными филиалами и представительствами. Иначе филиалы и представительства, удаленные от головной организации, оказываются изолированными от централизованных данных и ресурсов, либо располагают корпоративными информационными сервисами худшего качества. Управление бизнес процессами в рамках всей организации при этом затруднено из-за отсутствия единого информационного пространства. Дополнительным фактором, который в последнее время приходится учитывать при развитии вычислительной сети, является необходимость обеспечения безопасности информационных сервисов и защиты данных. Решением проблемы является создание частной региональной сети, объединяющей корпоративные вычислительные сети головного вуза, филиалов и представительств.

Доклад посвящен обобщению опыта перепроектирования корпоративной вычислительной сети (КВС) Владивостокского государственного университета экономики и сервиса (ВГУЭС) с использованием сетевой операционной системы Microsoft Windows 2000 Server (W2k) и технологии Active Directory (AD). Ядром AD является распределенная база данных, которая содержит средства синхронизации данных, находящихся на нескольких серверах сети (контроллерах доменов).

В логической структуре AD ВГУЭС используется один лес. Это, во-первых, позволяет использовать одни и те же групповые политики безопасности для ограничения пользователей находящихся в разных доменах, а, во-вторых, использовать механизмы адаптации логической структуры W2k к физической топологии корпоративной сети ВГУЭС, что позволяет повысить производительность вычислительной сети и некоторых сетевых сервисов.

На уровне доменов выделено четыре логические единицы. Первый домен (vvsu.ru) является родительским доменом по отношению к остальным доменам. В дальнейшем планируется использовать этот домен для установления доверительных отношений с доменами из других лесов (в рамках региональной академической сети с доменами других университетов и институтов ДВО РАН).

Второй домен (edu.vvsu.ru) используется для хранения учетных записей студентов и преподавателей университета, а также содержит информационные ресурсы, относящиеся к учебному процессу (корпоративные серверы, централизованное периферийное оборудование и т.п.). Внутренняя структура домена edu.vvsu.ru состоит из групп и подразделений, соответствующих институтам, кафедрам, группам студентов. Это позволяет упростить процесс администрирования (например, права на какой-либо ресурс могут быть делегированы сразу всей кафедре или институту).

Третий домен (emp.vvsu.ru) содержит учетные записи сотрудников университета, не являющихся преподавателями. Структура этого домена содержит подразделения и группы соответствующие административным и вспомогательным подразделениям вуза. Если сотрудник университета является одновременно и преподавателем, то для него заводится только одна учетная запись в зависимости от места основной работы. Подобные манипуляции с учетными записями пользователей допустимы, так как все учетные записи имеют уникальный идентификатор в рамках леса и все домены находятся в доверительных отношениях.

Четвертый домен (adm.vvsu.ru) отвечает за корпоративные сетевые ресурсы и используется для интеграции программных продуктов третьих фирм в W2k. Подобная интеграция позволит унифицировать процесс администрирования корпоративной сетью. К

примеру, активное сетевое оборудование Nortel Networks (во ВГУЭС используются коммутаторы BayStack 350/450, Accellar 1100), имеет возможность фильтрации трафика согласно групповым политикам, хранящимся в службе каталогов.

Все домены в рамках леса имеют двусторонние транзитивные отношения с родительскими и дочерними доменами. Так, например, пользователи домена emp.vvsu.ru часто обращаются к ресурсам домена adm.vvsu.ru, поэтому в целях повышения производительности AD необходимо обеспечить доверительные отношения между двумя этими доменами. Это позволит пользователям emp.vvsu.ru получать доступ к корпоративным ресурсам за два этапа, а не за три, что на треть сокращает время доступа к корпоративным ресурсам.

При проектировании физического уровня AD выполнен анализ объем предполагаемого трафика, генерируемого службами AD, и предложено организовать два узла в головном вузе (Владивосток) и по одному узлу на каждый филиал (Артем, Находка, Уссурийск). Узким местом в корпоративной сети головного вуза является магистральный канал, соединяющий два учебных корпуса. Снизить нагрузку на магистральный канал удалось за счет трех факторов: 1) AD имеет очень тонкий механизм настройки репликации данных между узлами 2) данные между узлами передаются в сжатом виде 3) при обращении рабочих станций к сетевым ресурсам они находят ближайший контроллер домена для прохождения авторизации. Расписание репликации данных AD выбрано таким образом, чтобы исключить возможность проведения синхронизации данных в периоды высокой загруженности контроллеров доменов. Предполагается, что нагрузка на контроллеры будет высокой в пятиминутном интервале после начала каждой пары. В этот период студенты одновременно будут проходить авторизацию на контроллерах домена edu.vvsu.ru (около 1500 рабочих станций). Адресное пространство сетевого уровня распределено таким образом, что компьютеры, относящиеся к одной IP-сети, находятся в одном здании. Т.к. планируется использовать по одному контроллеру домена edu.vvsu.ru в каждом узле, то рабочие станции будут использовать для авторизации контроллер домена, находящийся в том же здании что и рабочая станция, что значительно снизит нагрузку на магистральный канал.

Поддержка однотипного процесса авторизации пользователей в W2k и наличие специфицированного протокола LDAP (RFC 1777) для доступа к данным в хранилище позволила добавить ряд сервисов для удобства работы клиентов и упрощения работы администраторов корпоративной сети ВГУЭС. Реализован сервис, который выполняет автоматизированную регистрацию пользователей в AD. Для этого используется специализированный web-сайт университета, на котором любой пользователь может подать заявку на регистрацию. Программа проверит права данного пользователя на регистрацию в КВС, используя сведения в корпоративной базе данных управленческого учета, создаст учетную запись в AD и дерево каталогов на файловом сервере для данного пользователя. Поддерживается возможность использования плавающих профилей пользователя. Каталог файлового сервера, принадлежащий пользователю, автоматически подключается в качестве сетевого диска при регистрации пользователя в КВС. Еще один сервис реализует возможность управления доступом в Интернет клиентов корпоративной сети. Proxy-сервер взаимодействует с операционной системой W2k, и определяет учетную запись пользователя, который на данный момент использует Интернет. Таким образом, пользователю не требуется многократно вводить свой логин и пароль. Операции авторизации проходят абсолютно прозрачно для пользователя, а администратор имеет возможность управлять доступом к ресурсам Интернет на уровне конкретного пользователя.

Использование AD позволит обеспечить единый доступ пользователей региональной сети, в частности филиалов ВГУЭС, в локальную сеть университета, что сделает прозрачной работу с университетскими сервисами ранее доступными только в локальной сети. Общий доступ позволит создать единое информационное пространство, в котором возможно централизованное управление финансовыми, людскими и информационными потоками. Возможен доступ в локальную сеть и из других структур региональной сети (обеспечив доверительные отношения между лесами), что будет способствовать интеграции академических институтов и университетов региона, а также совместному использованию ресурсов.